

DE BRAUW
BLACKSTONE
WESTBROEK

Google violates Dutch Data Protection Act by combining user data

The Dutch data protection authority has found that Google's combining of user data is in violation of the Dutch Data Protection Act. The investigation gives you an insight into the requirements for the combination of (sensitive) user data.

This article is available in English only.

Google introduced its privacy policy on 1 March 2012, which states that Google can combine the personal data of data subjects collected across all of Google's services. Before Google's privacy policy was in effect, the French data protection authority had already initiated an investigation on behalf of all European data protection authorities (united in the Article 29 Working Party). The outcome of that initial investigation triggered six national data protection authorities, including the Dutch data protection authority (*College bescherming persoonsgegevens*; CBP), to start investigations based on their own national laws. On 28 November 2013, the CBP published the outcome of its investigation in its report of definitive findings.

Conclusion

The CBP found that:

- Google does not fulfil its obligation under the Dutch Data Protection Act (*Wet bescherming persoonsgegevens*; DDPA) to provide clear and sufficient information
- Google's purposes for combining user data are not specific and legitimate
- Google has no legal ground for combining user data.

Obligation to inform

The CBP concluded that Google does not fulfil its obligation to provide clear and sufficient information to data subjects (i) about its identity, and (ii) the purposes for which data subjects' personal data are processed. The CBP states three reasons for reaching that conclusion:

- Google does not provide sufficient information about its identity as a data controller on the YouTube website
- where Google does provide information to data subjects, the information is fragmented and irregular
- Google does not provide sufficiently specific information about the types of personal data that are processed and the purposes for which Google combines these data.

Ambiguous and insufficiently specific purposes

Google's privacy policy states four purposes for which Google combines user data:

- personalisation of services requested
- product development
- display of personalised ads
- website analytics

According to the CBP, these purposes are ambiguous and insufficiently specific. As personal data has to be processed for explicit, sufficiently specified and legitimate purposes in order for the processing to be legitimate under the DDPA, the CBP concluded that Google violates the DDPA.

No legal ground

In order for combining user data to be legitimate, Google requires a legal ground under the DDPA. During the investigation, Google stated that it has legal grounds for combining user data based on:

- the unambiguous consent of data subjects (section 8 (a) DDPA)
- the necessity for the performance of a contract between Google and data subjects (section 8 (b) DDPA)
- Google's legitimate interest (section 8 (f) DDPA).

The CBP concluded, however, that none of these legal grounds is applicable to Google's combining of user data.

Unambiguous consent

As Google often collects personal data with the aid of tracking cookies, the CBP concluded that Google is required to obtain data subjects' prior informed consent. The CBP found, however, that Google does not offer data subjects any (prior) options to consent or reject their data being combined. In that light, Google stated that data subjects gave their unambiguous consent for their user data being combined by accepting Google's general terms of service and privacy policy. The CBP, in contrast, concluded that unambiguous consent cannot be obtained through general terms of service because data subjects have to be informed and consent has to be specific.

Performance of a contract

Google argued that combining user data was necessary for the performance of a contract between Google and data subjects, since Google's terms of service create a contractual relationship with all users of Google's services. The CBP disagreed with Google and concluded that this legal ground is not applicable because:

- Google requires unambiguous consent due to the use of tracking cookies
- there is no justification for combining user data in Google's relationship with specific individual data subjects (or any agreement entered into with them).

In this regard, the CBP placed special attention to the fact that passive users of Google (i.e., users that do not have a Google account) will not be subject to Google's terms of service

and often may not even be aware that they have encountered Google cookies while using a third-party website.

Legitimate interest

The CBP concluded that Google had not convincingly shown that its combining user data outweighs the data subject's right to the protection of its privacy, based on:

- the sometimes sensitive nature of the processed personal data;
- the diversity of Google's services;
- the lack of adequate and specific information
- the lack of effective opt-outs.

The CBP added that the personal data collected are sometimes of a sensitive nature (e.g., payment information, data location and information about surfing behaviour) and that Google offers very diverse services which serve entirely different purposes in the users' view (e.g., email, consulting maps, viewing videos). Combined with the fact that Google does not provide adequate and specific information and that Google does not have adequate safeguards in place (e.g., effective opt-outs), the data subject's right to protection of its privacy prevails over Google's legitimate interest. Google's market share in the Netherlands also played an important role in the CBP's assessment since it is almost impossible for Dutch users to not interact with Google.